

## § 75.114

there is a loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The term “unauthorized access” used in the definition of “data breach” includes access to an electronic information system and includes, but is not limited to, viewing, obtaining, or using data containing sensitive personal information in any form or in any VA information system. The phrase “unauthorized access incidental to the scope of employment” includes instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information. Accordingly, an unauthorized access, other than an unauthorized access incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data, constitutes a data breach. In addition to these circumstances, VA also interprets data breach to include circumstances in which a user misuses sensitive personal information to which he or she has authorized access. The following circumstances do not constitute a data breach and, consequently, are not subject to the provisions of this subpart:

(a) An unauthorized access to data containing sensitive personal information that was determined by the Secretary to be incidental to the scope of employment, such as an inadvertent unauthorized viewing of sensitive personal information by a VA employee or a person acting on behalf of VA.

(b) A loss, theft, or other unauthorized access to data containing sensitive personal information that the Secretary determined to have no possibility of compromising the confidentiality or integrity of the data, such as the inability of compromising the confidentiality or integrity of the data because of encryption or the inadvertent disclosure to another entity that is re-

## 38 CFR Ch. I (7–1–10 Edition)

quired to provide the same or a similar level of protection for the data under statutory or regulatory authority.

(Authority: 38 U.S.C. 501, 5724, 5727)

### § 75.114 Accelerated response.

(a) The Secretary, in the exercise of his or her discretion, may provide notice to records subjects of a data breach and/or offer them other credit protection services prior to the completion of a risk analysis if:

(1) The Secretary determines, based on the information available to the agency when it learns of the data breach, that there is an immediate, substantial risk of identity theft of the individuals whose data was the subject of the data breach, and providing timely notice may enable the record subjects to promptly take steps to protect themselves, and/or the offer of other credit protection services will assist in timely mitigation of possible harm to individuals from the data breach; or

(2) Private entities would be required to provide notice under Federal law if they experienced a data breach involving the same or similar information.

(3) In situations described in paragraphs (a)(1) or (a)(2) of this section, the Secretary may provide notice of the breach prior to completion of a risk analysis, and subsequently advise individuals whether the agency will offer additional credit protection services upon completion, and consideration of the results, of the risk analysis, if the Secretary directs that one be completed.

(b) In determining whether to promptly notify individuals and/or offer them other credit protection services under paragraph (a)(1) of this section, the Secretary shall make the decision based upon the totality of the circumstances and information available to the Secretary at the time of the decision, including whether providing notice and offering other credit protection services would be likely to assist record subjects in preventing, or mitigating the results of, identity theft based on the compromised VA sensitive personal information. The Secretary's exercise of this discretion will be based on good cause, including consideration of the following factors:

## Department of Veterans Affairs

## § 75.116

(1) The nature and content of the lost, stolen or improperly accessed data, e.g., the data elements involved, such as name, social security number, date of birth;

(2) The ability of an unauthorized party to use the lost, stolen or improperly accessed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects, if able to access and use the data;

(3) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(4) Ease of physical access to the lost, stolen or improperly accessed data, e.g., the degree to which the data is readily available to unauthorized access, such as being in a dumpster readily accessible by members of the general public;

(5) The format of the lost, stolen or improperly accessed data, e.g., in a standard electronic format, such as ASCII, or in paper;

(6) Evidence indicating that the lost, stolen or improperly accessed data may have been the target of unlawful acquisition; and

(7) Evidence that the same or similar data had been acquired from other sources improperly and used for identity theft.

(c) VA will provide notice and/or other credit protection services under this section as provided in §§ 75.117 and 75.118.

(Authority: 38 U.S.C. 501, 5724, 5727)

### § 75.115 Risk analysis.

If a data breach involving sensitive personal information that is processed or maintained by VA occurs and the Secretary has not determined under § 75.114 that an accelerated response is appropriate, the Secretary shall ensure that, as soon as possible after the data breach, a non-VA entity with relevant expertise in data breach assessment and risk analysis or VA's Office of Inspector General conducts an independent risk analysis of the data breach. The preparation of the risk analysis may include data mining if necessary for the development of rel-

evant information. The risk analysis shall include a finding with supporting rationale concerning whether the circumstances create a reasonable risk that sensitive personal information potentially may be misused. If the risk analysis concludes that the data breach presents a reasonable risk for the potential misuse of sensitive personal information, the risk analysis must also contain operational recommendations for responding to the data breach. Each risk analysis, regardless of findings and operational recommendations, shall also address all relevant information concerning the data breach, including the following:

(a) Nature of the event (loss, theft, unauthorized access).

(b) Description of the event, including:

(1) Date of occurrence;

(2) Data elements involved, including any personally identifiable information, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(6) Time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); and

(8) Known misuses of data containing sensitive personal information, if any.

(c) Assessment of the potential harm to the affected individuals.

(d) Data breach analysis, as appropriate.

(Authority: 38 U.S.C. 501, 5724, 5727)

### § 75.116 Secretary determination.

(a) Upon receipt of a risk analysis prepared under this subpart, the Secretary will consider the findings and other information contained in the risk analysis to determine whether the data breach caused a reasonable risk for the potential misuse of sensitive personal